DRAFT

Chuck Fairbrook - (OSD)

...TIONAL SECURITY DECISION

DIRECTIVE NO._____

NATIONAL POLICY ON TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS SECURITY

This Directive provides the policy, objectives and principles to guide the conduct of national activities directed toward properly safeguarding national security and government-held privacy information which is processed or communicated by electronic means.

Telecommunications and electronic information processing systems if not equipped and operated so as to deny or thwart the applicable threat, are highly susceptible to interception and other unauthorized exploitation. The technology to exploit electronic systems is widespread and is used extensively by the Warsaw Pact nations as well as by terrorist groups and radical elements. Assuring the security integrity of systems used to process and communicate national security and privacy information is a national responsibility.

1. Objectives. To fulfill these responsibilities, I direct that the nation's capabilities for securing telecommunication and automated information systems against technical exploitation threats be maintained and improved as necessary to provide for:

a. A superior technical base, both within government and industry.

b. A reliable and continuing capability to assess threats and to implement appropriate, effective countermeasures.

c. Support of other policy objectives for national telecommunications and automated information resources.

d. Effective use of applicable resources.

2. Principles: In support of these objectives, the following policy principles are established:

a. Systems which generate, store, process or transmit classified information in electrical form shall be secured or protected by such means necessary to prevent technical exploitation.

b. Systems similarly handling other government-derived information, the loss of which could adversely affect the national interest or the rights of U.S. persons, shall be protected in proportion to the cost of the loss of such information if the applicable threat of technical exploitation were successful.

c. Systems which handle non-government information of similar nature should be protected commensurate with the threat of exploitation and at a cost not to exceed the value of the potential loss of such information. The Government shall take necessary steps to identify such systems and information and formulate strategies and measures for providing protection. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-governmental systems would be in the national interest, the private sector shall be encouraged to undertake the application of such measures.

3. Implementation. A steering Group consisting of the Executive Agent for Communications Security, the Director of Central Intelligence, the Associate Director of the Office of Management and Budget (OMB) for National Security and International Affairs, and chaired by the Assistant to the President for National Security Affairs, or his representative, is established. The Steering Group shall:

a. Oversee this Directive and ensure its implementation. It shall provide guidance to the Director, National Security Agency with respect to the activities consistent with this Directive.

b. Monitor the ongoing activities of the National Telecommunications and Information Systems Security Committee with respect to the objectives and policy elements stated herein.

c. Review and approve consolidated resources program and budget proposals, and other matters referred to it by the Executive Agent in fulfillment of responsibilities outlined in subparagraph (4), below.

d. Annually review and evaluate the security status of national telecommunications and automated information systems with respect to established objectives and priorities.

e. Interact with the Steering Group on National Security Telecommunications and, through that Group, with the National Security Telecommunications Advisory Committee (NSTAC), to ensure that the objectives and policy elements of this Directive are addressed.

f. Recommend for Presidential approval additions or revisions to this Directive as national interests require.

4. The National Telecommunications and Information Systems Security Committee.

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is hereby established and will operate under the direction of the Systems Security Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be composed of a representative of each of the following:

The Secretary of Defense (non-voting)

The Secretary of State

The Secretary of the Treasury

The Secretary of Energy

The Secretary of Transportation

The Attorney General

The Secretary of Commerce

The Director, Office of Management and Budget

The Chief of Staff, United States Army

The Chief of Naval Operations

The Chief of Staff, United States Air Force

The Chairman, Joint Chiefs of Staff

The Director, Central Intelligence Agency

The Director, Federal Emergency Management Agency

The Administrator, General Services Administration

The Manager, National Communications System

The Director, National Security Agency

b. The Committee shall:

(1) Establish such specific operating policies, objectives, and priorities as may be required to implement this Directive.

(2) Submit to the Steering Group an annual evaluation of the status of national telecommunications and information security with respect to established objectives and priorities.

(3) Administer matters pertaining to the release of sensitive security information, techniques, and materials to foreign governments or international organizations.

(4) Establish and maintain a national issuance system for promulgating the operating policies, directives and guidance which may be issued pursuant to this Directive.

(5) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities.

c. The Committee shall make recommendations to the Steering Group on Committee membership and may establish criteria and procedures for permanent observers. Representatives of other departments or agencies affected

by specific matters under deliberation will attend upon invitation of the Chairman.

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency. The secretariat may be augmented as necessary by personnel provided by the Departments and Agencies represented on the Board in response to the Chairman's request. The National Security Agency shall provide facilities and support as required.

5. The Executive Agent of the Government for Communications Security.

The Secretary of Defense is the Executive Agent of the Government for Communications Security. In this capacity he shall serve an expanded role to act within policies and procedures established by the Steering Group and the NTISSC to:

a. Ensure the development, in conjunction with Director, National Security Agency and with NTISSC member Departments and Agencies, of plans to fulfill the objectives of this Directive, including the formulation of necessary security architectures.

b. Fulfill requirements of the Federal Government for technical security material and related services.

c. Provide or approve security standards and doctrine.

d. Conduct or approve research and development of security techniques and equipment.

e. Operate or coordinate the efforts of Government technical centers related to telecommunications and automated information systems security.

f. Develop and submit to the Steering Group and the Congress a proposed National Telecommunications and Information Systems Security Program budget for each fiscal year.

6. The Director, National Security Agency.

The Director, National Security Agency is responsible for executing the foregoing responsibilities of the Secretary of Defense as Executive Agent. In fulfilling these responsibilties he shall have authority to:

a. Empirically examine federal telecommunications and associated electronic information handling systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with the law and other applicable directives.

b. Act as the single government focal point for all matters related to cryptography to include; conducting research and development; prescribing or approving all standards, techniques, systems and equipments; and conducting liaison with foreign governments, international organizations, and private institutions.

c. Operate such industrial facilities as may be required to perform critical functions related to the provision of cryptographic and other sensitive security materials or services.

d. Operate a central technical center(s) to assess and disseminate information on hostile threats to national telecommunications and information systems security.

e. Operate a central technical center(s) to evaluate the security of telecommunications systems, computer systems and data networks, and to conduct or sponsor research and development of security techniques.

f. Prescribe the control systems and standards for protecting cryptographic and other sensitive security material, techniques, and information.

7. The Director of Central Intelligence shall identify to the NTISSC and the Director, NSA, as appropriate, any unique handling requirements associated with the protection of sensitive compartmented intelligence.

8. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue such standards for the security of telecommunications and other electronic information resources as the Director, NSA may approve and authorize for public release in accordance with authorities assigned herein.

9. The Director, Office of Management and Budget shall review for consistency with this Directive, and amend as appropriate, OMB Circulars A-71

(Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein.

10. The Heads of Federal Departments and Agencies shall:

a. Conform with any policies, standards and doctrines issued by proper authority pursuant to this Directive.

b. Provide to the Systems Security Steering Group, the NTISSC, the Secretary of Defense as Executive Agent, and the Director, National Security Agency such information as they may require to discharge responsibilties assigned herein.

11. Nothing in this Directive shall:

a. Alter the existing authorities of the Director of Central Intelligence for the overall direction, coordination and supervision of intelligence matters, nor his responsibilitity to act as Executive Agent of the Government for technical security countermeasures (TSCM) against bugging, eavesdropping and related forms of surveillance.

b. Give the NTISSC, the Secretary of Defense, or the Director, National Security Agency authority to inspect the personnel, facilities, or internal operations of other departments and agencies without their approval. This provision does not constrain the authority of the Director, NSA to monitor telecommunications or the emissions of other electronic information systems consistent with paragraph 11.a., above.

c. Amend or contravene the provisions of other, existing directives which may pertain to the financial management of automated information resources or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

12. For the purposes of this Directive, the following terms shall have the meanings indicated.

a. Telecommunications means the creation, preparation, manipulation, transmission, communication or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

b. Automated Information Systems means systems which created, prepare, manipulate or process information in electronic form for purposes other than telecommunication, and includes computers, word processing systems and associated equipment.

c. Telecommunications and Information Systems Security means protection afforded to telecommunications, automated information systems, and other electronic information handling systems in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, handle, or process information of use to an adversary, and also includes physical protection of sensitive security resources and materials.

13. PD/NSC-24 is hereby superseded.